REMARKS

Applicants respectfully request favorable reconsideration of this Application, as amended.

Applicants again acknowledge, with appreciation, the indication of allowable subject matter in Claims 15 and 16.

By this Amendment, Claims 14, 16, and 17 have been amended for clarity of expression and to clarify the invention intended to be claimed. Applicants previously cancelled Claims 1-13 without prejudice or disclaimer. Thus, Claims 14-34 are pending.

In the outstanding Office Action, Claims 14 and 34 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,304,658 to Kocher et al. ("*Kocher*"); Claims 17, 18, 21-27, 31, and 32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kocher* in view of Menezes et al., "Handbook of Applied Cryptography" ("*Menezes*") and further in view of U.S. Patent No. 6,411715 to Liskov ("*Liskov*"); Claims 28-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kocher* and *Menezes*, and further in view of Stinson, "Cryptography Theory and Practice" ("*Stinson*"); and Claims 19 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kocher* and *Menezes*, and further in view of U.S. Patent No. 6,202,933 to Poore et al. ("*Poore*"). These rejections are respectfully traversed.

To anticipate a claim, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989); MPEP § 2131.

Here, independent Claim 14 recites, *inter alia*, a method for verifying a signature or an authentication including, for example, retrieving a prevalidation value by a smart card and using a second computing means to perform at least one modular reduction by utilizing the prevalidation value to obtain the remainder of a modulo n calculation, without any division operation at the level of the smart card. It is apparent that none of the applied references teach or suggest at least this feature of Claim 14.

For example, *Kocher* clearly states, in contrast to Claim 14, that "[a]t step 315, the device updates z again by computing z←z/k. (There should be no remainder from this operation, since k divides z.)." *See Kocher*, col. 16, lines 6-7 (underline added). *Kocher* thus clearly teaches performing a division operation in the device (token). It is therefore apparent that *Kocher* does not teach or suggest "retrieving said prevalidation value by the smart card and using said second computing means to perform at least one modular reduction by utilizing said prevalidation value to obtain the remainder of the modulo n calculation, without any division operation at the level of the smart card" as recited in Claim 14.

Furthermore, Applicants also respectfully disagree with the assertions made in the "Response to Arguments" section of the Office Action. (*See* Office Action at 2-3.) First, the Office Action alleges that "A' is similar to M'...which includes q quotient of a modulo n calculation. And...Figure 3 shows a process of authentication comprising a calculation process by transmitting information back and forth between two parties, wherein the output of R' (335) is transferred back to the sender for further process." *Id.* Applicants respectfully disagree. In contrast, *Kocher* clearly teaches that the values of either A' or M' are not sent by the server to the token. *See Kocher*,

Figure 1 (125 to 130); Figure 3 (303). Moreover, as can be seen in Figure 3 of *Kocher*, contrary to the assertion in the Office Action, R' is not sent back to the sender, but, rather, is merely used to calculate d_2. *See Kocher*, Figure 3 (340). Thus, *Kocher* also fails to teach or suggest an electronic communication means of the terminal transmitting to the smart card said response data comprising at least a prevalidation value, where the prevalidation value represents at least a quotient of a modulo n calculation, as recited in Claim 14.

Therefore, Applicants respectfully submit that independent Claim 14 patentably distinguishes from *Kocher*. Furthermore, it is also apparent that *Menezes, Liskov*, *Stinson*, and *Poore*, whether taken alone or in combination, fail to cure the above-discussed deficiencies of *Kocher*. Thus, Claims 15-34 are also believed to be patentable due to their dependence from independent Claim 14, as well as for the additional features recited in Claims 15-34.

In view of the foregoing, Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully requested.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance; the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2146-906752) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

MILES & STOCKBRIDGE, P.C.

By: _____

Edward J. Kondracki
Reg. No. 20,604

Eric G. King
Reg. No. 42,736

1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone: (703) 610-8647
4847-7433-7537